

I. Amendments to the Claims

This listing of claims replaces without prejudice all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for a provider to verify a client's secret identifier, comprising the steps of:
the client scrambles his/her predetermined secret identifier in a one-time, true random way with random data, to produce scrambled data comprising randomly interleaved (i) said secret identifier and (ii) said one-time, true random data;
the scrambled data is transmitted to the provider; and
the provider determines whether the client's secret identifier is present in the received scrambled data.
2. (Previously Presented) A method in accordance with Claim 1, wherein the provider rejects a transaction if the random data in the received scrambled data is substantially the same as random data received in a previous transaction corresponding to said client.

3. (Currently Amended) A method for a provider to verify a client's secret identifier received in scrambled data which includes the secret identifier randomly interleaved with one-time, true random data, comprising the steps of:

determining whether the client's secret identifier is present in the received scrambled data, which includes the secret identifier randomly interleaved with the one-time, true random data;

comparing the one-time, true random data in the received scrambled data with previously received random data corresponding to said client; and

authorizing a transaction if the one-time, true random data in the received scrambled data is substantially different from said previously received random data.

4. (Currently Amended) Apparatus for a provider to verify a client's secret identifier, comprising:

means for the client to scramble his/her predetermined secret identifier in a one-time, true random way with one-time, true random data, the scrambled data consisting of randomly ~~interleave~~ interleaved (i) random data and (ii) the secret

identifier;

a transmitter which transmits the scrambled data to the provider; and

a provider processor which is used to determine whether the client's secret identifier is present in the received scrambled data.

5. (Previously Presented) Apparatus in accordance with Claim 4, wherein the provider processor rejects a transaction if the random data in the received scrambled data is substantially the same as random data received in a previous transaction corresponding to said client.

6. (Currently Amended) A process for a consumer to submit secure verification information, comprising the steps of:

obtaining a secret identifier from a provider, said secret identifier being unique to said consumer;

randomly interleaving, in a one-time truly random way, the consumer's secret identifier with a plurality of randomly selected alphanumeric characters; and

submitting the combined randomly interleaved secret identifier and plurality of randomly selected alphanumeric characters to the provider.

7. (Previously Presented) A process according to Claim 6, wherein said submitting step is performed on the Internet.

8. (Previously Presented) A process according to Claim 6, wherein said a randomly interleaving step and said submitting step are performed on a computer network.

9. (Previously Presented) A process according to Claim 6, wherein said randomly interleaving step and said submitting step are performed on a building security system.

10. (Previously Presented) A process according to Claim 6, wherein said submitting step is performed over a telephone system.

11. (Previously Presented) A process according to Claim 6, wherein said randomly interleaving step and said

submitting step are performed in a credit or debit card verification system.

12. (Previously Presented) A process according to Claim 6, wherein said randomly interleaving step and said submitting step are performed in an ATM system.

13. (Previously Presented) A process according to Claim 6, wherein said randomly interleaving step and said submitting step are performed in an phone card system.

14. (Previously Presented) A process according to Claim 6, wherein the consumer manually performs said randomly interleaving step.

15. (Previously Presented) A process according to Claim 6, further comprising the step of the provider rejecting the submitted randomly interleaved identifier if the randomly interleaved identifier is substantially identical to a randomly interleaved identifier previously submitted to the provider.

16. (Previously Presented) A process according to Claim 6, wherein the randomly interleaving step includes the step of changing an order of alphanumeric characters in the secret identifier.

17. (Currently Amended) A method of transacting a charge card purchase, comprising the steps of:

providing a user with a transaction form;

receiving from the user a credit card number and a super identifier, the super identifier comprising (i) a secret identifier unique to the user and (ii) a plurality of randomly chosen alphanumeric characters, selected in a one-time true random way, the super identifier comprising the randomly chosen alphanumeric characters randomly interleaved, in a one-time true random way, with the secret identifier;

comparing the received super identifier with a plurality of previously received super identifiers; and

accepting the credit card transaction if the received super identifier is not substantially identical to previously received super identifiers.

18. (Previously Presented) A method according to Claim 17, wherein the charge card purchase comprises a credit card purchase.

19. (Previously Presented) A method according to Claim 17, wherein the charge card purchase comprises a debit card purchase.

20. (Previously Presented) A method according to Claim 17, wherein the charge card purchase comprises a phone card purchase.

21. (Previously Presented) A method according to Claim 17, wherein the charge card purchase comprises a lottery ticket purchase.

22. (Previously Presented) A method according to Claim 17, wherein the secret identifier comprises a PIN.

23. (Previously Presented) A method according to Claim 17, wherein the randomly chosen alphanumeric characters are chosen by the user.

24. (Previously Presented) A method according to Claim 17, wherein the number of randomly chosen alphanumeric characters are the same as the number of characters in the secret identifier.

25. (Previously Presented) A method according to Claim 17, wherein the method is performed at a point of sale.

26. (Previously Presented) A method according to Claim 17, wherein the method is performed at a provider server.

27. (Previously Presented) A method according to Claim 17, wherein the method is performed over the Internet.

28. (Previously Presented) A method according to Claim 17, wherein the secret identifier is scrambled by the user using the plurality of alphanumeric characters.

29. (Currently Amended) A method of carrying out a secure financial transaction, comprising the steps of:

receiving from a user (i) a request for a transaction and (ii) a super PIN which comprises a PIN randomly interleaved, in a one-time true random way, with a plurality of alphanumeric characters randomly chosen, in a one-time true random way, by a user; and

accepting ~~rejecting~~ the request if the received super PIN is substantially different from ~~similar to~~ a previously received super PIN.

30. (Currently Amended) A method according to Claim 29, wherein the acceptance ~~rejection~~ criteria is dependent on the Super PIN ~~not~~ including all of the alphanumeric characters that comprise the user's secret identifier.

31. (Currently Amended) A method according to Claim 29, wherein the acceptance ~~rejection~~ criteria is dependent on the Super PIN not including substantially all of the plurality of randomly selected alphanumeric characters from a previous transaction.

32. (Previously Presented) A method according to Claim 29, where the previously used plurality of randomly selected alphanumeric characters are stored.

33. (Previously Presented) A method according to Claim 29, where a ~~the~~ rejection of the Super PIN validation triggers a supplementary validation activity.

34. (Currently Amended) Apparatus for a consumer to submit secure verification information including a secret identifier obtained from a provider, said a secret identifier being unique to said consumer, said apparatus comprising:

means for randomly interleaving, in a one-time true random way, the consumer's secret identifier with a plurality of alphanumeric characters; and

means for submitting the randomly interleaved identifier to the provider.

35. (Previously Presented) Apparatus according to Claim 34, wherein said means for submitting are coupled to the Internet.

36. (Previously Presented) Apparatus according to Claim 34, wherein said means for submitting are coupled to a computer network.

37. (Previously Presented) Apparatus according to Claim 34, wherein said means for submitting are coupled to a building security system.

38. (Previously Presented) Apparatus according to Claim 34, wherein said means for submitting are coupled to a telephone system.

39. (Previously Presented) Apparatus according to Claim 34, wherein said means for submitting are coupled to a credit card verification system.

40. (Previously Presented) Apparatus according to Claim 34, wherein said means for submitting are coupled to an ATM system.

41. (Currently Amended) Apparatus according to Claim 34, wherein the consumer uses a writing instrument to manually perform ~~performs~~ the random interleaving.

42. (Previously Presented) Apparatus according to Claim 34, wherein an automated process or device performs the random interleaving.

43. (Previously Presented) Apparatus according to Claim 34, wherein an automated process or device creates the Super PIN on behalf of the user.

44. (Currently Amended) Apparatus according to Claim 34, further comprising a provider server for rejecting the submitted randomly interleaved identifier if the randomly interleaved ~~interleaving~~ identifier is substantially identical to a randomly interleaved ~~interleaving~~ identifier previously submitted to the provider.

45. (Previously Presented) Apparatus according to Claim 34, wherein the means for randomly interleaving includes means for changing an order of alphanumeric characters in the secret identifier.

46. (Currently Amended) Apparatus for transacting a charge card transaction, comprising:

means for receiving from the user a credit card number and a super identifier, the super identifier comprising (i) a secret identifier unique to the user and (ii) a plurality of randomly chosen alphanumeric characters, said super identifier comprising the plurality of randomly chosen alphanumeric characters randomly interleaved, in a one-time true random way, with said secret identifier;

means for comparing the received super identifier with a plurality of previously received super identifiers; and

means for accepting the credit card transaction if the received super identifier is not substantially identical to previously received super identifiers.

47. (Previously Presented) Apparatus according to Claim 46, wherein the secret identifier comprises a PIN.

48. (Currently Amended) Apparatus according to Claim 46, wherein the randomly chosen alphanumeric characters are chosen by the user in a one-time true random way.

49. (Previously Presented) Apparatus according to Claim 46, wherein the number of randomly chosen alphanumeric characters are the same as the number of characters in the secret identifier.

50. (Previously Presented) Apparatus according to Claim 46, wherein said means for receiving are disposed at a point of sale.

51. (Previously Presented) Apparatus according to Claim 46, wherein said means for receiving are disposed at a provider server.

52. (Previously Presented) Apparatus according to Claim 46, wherein said means for receiving are coupled to the Internet.

53. (Previously Presented) Apparatus according to Claim 46, wherein the secret identifier is interleaved by the user using the plurality of alphanumeric characters.

54. (Currently Amended) Apparatus for carrying out a secure financial transaction, comprising:

means for receiving from a user (i) a request for a transaction and (ii) a super PIN which comprises a PIN randomly interleaved, in a one-time true random way, with a plurality of alphanumeric characters randomly chosen by a user; and

means for accepting ~~rejecting~~ the request if the received super PIN is substantially dissimilar ~~similar~~ to a previously received super PIN.

55. (Previously Presented) A method according to Claim 1, wherein at least one of the secret identifier and the random data comprises a sequence of alphanumeric symbols.

56. (Previously Presented) Apparatus according to Claim 4, wherein at least one of the secret identifier and the random data comprises a sequence of alphanumeric symbols.

57. (Previously Presented) A method according to Claim 28, wherein at least one of the secret identifier and the random data comprises a sequence of alphanumeric symbols.

58. (Previously Presented) Apparatus according to Claim 54, wherein at least one of the secret identifier and the random data comprises a sequence of alphanumeric symbols.